Legislative Audit Division

State of Montana

Report to the Legislature

May 2005

Information System Audit

Computer Disposal Policy

While testing the effectiveness of the State's policy on disposal of computers, we viewed sensitive and confidential information remaining on surplused computers, that agencies did not remove in accordance with state policy.

Direct comments/inquiries to:
Legislative Audit Division
Room 160, State Capitol
PO Box 201705
Helena MT 59620-1705

04SP-31

Help eliminate fraud, waste, and abuse in state government. Call the Fraud Hotline at 1-800-222-4446 statewide or 444-4446 in Helena.

INFORMATION SYSTEM AUDITS

Information System (IS) audits conducted by the Legislative Audit Division are designed to assess controls in an IS environment. IS controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. In performing the audit work, the audit staff uses audit standards set forth by the United States Government Accountability Office.

Members of the IS audit staff hold degrees in disciplines appropriate to the audit process. Areas of expertise include business, accounting and computer science.

IS audits are performed as stand-alone audits of IS controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

MEMBERS OF THE LEGISLATIVE AUDIT COMMITTEE

Senator John Cobb	Representative Dee Brown
Senator Mike Cooney	Representative Tim Callahan
Senator Jim Elliott, Acting Chair	Representative Hal Jacobson
Senator John Esp	Representative Scott Mendenhall
Senator Dan Harrington	Representative John Musgrove
Senator Corey Stapleton	Representative Rick Ripley

LEGISLATIVE AUDIT DIVISION

Scott A. Seacat, Legislative Auditor
John W. Northey, Legal Counsel

Deputy Legislative Auditors:
Jim Pellegrini, Performance Audit
Tori Hunthausen, IS Audit & Operations
James Gillett, Financial-Compliance Audit

May 2005

The Legislative Audit Committee
of the Montana State Legislature:

This report is a description of our Information Systems audit, its purpose, methods and results. Our work focused on the Computer Disposal Policy and its effectiveness in keeping citizen, state and federal information private.

The report contains one recommendation to address the effectiveness of existing policy.

We wish to express our appreciation to the Department of Administration and respective state agencies whose computers were a part of testing, for their cooperation and assistance during this project.

Respectfully submitted,

(Signature on File)

Scott A. Seacat
Legislative Auditor

Room 160, State Capitol Building PO Box 201705 Helena, MT 59620-1705
Phone (406) 444-3122 FAX (406) 444-9784 E-Mail lad@state.mt.us

Legislative Audit Division

Information System Audit

Computer Disposal Policy

Members of the audit staff involved in this audit were David Nowacki and Dale Stout.

Table of Contents

Appointed and Administrative Officials

Department of Administration	Janet Kelly, Director
	Jeff Brandt, Acting Chief Information Officer
	Kyle Hilmer, Policy & Planning Services Bureau Chief

Executive Summary

Background

Much of state government's business is conducted using computers which work with and store private or disclosure restricted information.

The Montana Constitution affirms Montana citizens' right of privacy and the state's duty to protect this privacy. Implementing this right through statute and policy, the state is required to protect individual privacy and the privacy of the information contained within the computer systems by restricting information disclosure.

Government information managers have recognized the risk of information disclosure and require all information be removed before a state agency disposes of computers. The resulting state computer disposal policy requires, "All agency data must be removed from the computer in such a manner that it cannot be recovered" when the disposal computer leaves an agency.

Audit Objective

To test the effectiveness of the computer disposal policy, we acquired computer hard drives from computers no longer used for state business, and determined whether all data and software were removed in accordance with state policy.

Scope and Methodology

There were 51 state agencies disposing in excess of 2,300 computers during calendar year 2004. We acquired 18 computer hard drives from these computers, originating from eight different state agencies. We examined each hard drive for recoverable information. If no information was present, we concluded the agency had met state policy and properly removed information. If any information was recovered, we concluded the agency had not met state policy requirements.

- We were able to recover information on 12 of the 18 hard drives we acquired.
- Eight of the 18 hard drives held information restricted from public disclosure by Montana's constitution, legal statutes, administrative rules or Federal requirements.

Executive Summary

Summarization

Removing all information from computers no longer needed for state business is an effective method enabling the state to meet its information privacy responsibilities. The following report includes one recommendation to address the state's lack of a single clear policy instructing departments on information removal, and the communication of responsibility for data removal.

Chapter I - Information Privacy and Computers

Introduction

Nearly every desktop computer in use today contains one or more hard drives. A hard drive (drive) stores information in a relatively permanent form. Significant amounts of data are stored on a desktop computer's hard drive. When data is "erased," the data remains on the drive unless effectively overwritten or the drive physically destroyed. If not overwritten or destroyed, data can be recovered using readily available software.

Privacy

Effective July 1, 2001 Montana established in law, the "Montana Information Technology Act." Within the act, Montana's information technology policy recognizes individual privacy and the privacy of information contained within information technology systems.

Privacy is an individual's inherent right. The Montana Constitution confirms this expectation and affirms Montana citizens' right of privacy and the state's duty to protect this privacy. Implementing this right through statute and policy, the state is required to protect individual privacy and the privacy of the information contained within computer systems by restricting information disclosure.

Privacy Risks

State agencies are directed to improve government by aggressively deploying electronic service delivery to citizens and accommodating electronic transmissions between Montana citizens, state government and businesses. To meet this objective, state government has significantly computerized government operations. Montana's government agencies now operate approximately 11,000 computers. A challenge is balancing privacy risks, such as unintended information disclosure, with increased efficiency gained by using computers. One such risk is the sensitivity of the data residing in storage, and the disposition of that data when an agency disposes of a computer or transfers a computer to another entity. To address this risk, the Department of Administration has implemented policy for disposal of computers, dated June 2003.

Chapter I – Information Privacy and Computers

Policy Interpretation

State policy specifies **all** agency information should be removed in such a way that meaningful information cannot be recovered from the computer's hard drive (emphasis added). In other words, the hard drive should be "empty," containing no recognizable information.

We interpreted the word "recovered" means information is retrieved from the hard drive. We interpreted "meaningful" information to be any information capable of being understood through reading, viewing (pictures, graphs, icons for example) or hearing (music or voice recordings for example). In other words, if someone can read, view, or hear information and can make sense of it, information storage has not been properly "removed."

Project Objective

To test the effectiveness of the computer disposal policy, we acquired hard drives from computers no longer used for state business, to determine whether all data and software were removed in accordance with state policy.

Project Scope and Methodology

There were fifty-one state agencies disposing in excess of 2,300 computers during 2004. We acquired 18 hard drives from computers originating from eight state agencies and tested for data removal. We acquired six state computers the same way the public can acquire these computers; we bought them from the state. We acquired 12 computers the same way public schools can acquire these computers; we borrowed donated computers. We selected one of the many readily available tools created specifically for reading or recovering information from the computer's hard drive.

Our work was conducted in accordance with government auditing standards as established by the Government Accountability Office.

Chapter II – Computer Disposal Policy Effectiveness

Background

As computers reach the end of their useful life or computing requirements change, state agencies remove computers from service and dispose of them. Currently, agencies dispose of computers in the following ways:

- Transfer to other state agencies;
- Sell to the public via the state surplus property program;
- Donate to Montana school districts via the Office of Public Instruction (OPI); or
- Discard in landfills.

Since 1997, approximately 5,700 computers have been donated by state agencies to Montana school districts. Fewer computers are sold to the public or transferred to other agencies and only non-operational computers or parts are sent to landfills.

Current Computer Disposal Policy Needs Clarification

When disposing of a computer, including transferring a computer to the surplus property program or to OPI, there is a state policy requirement on data removal. The policy as currently written is not adequate to meet its stated purpose "to ensure that sensitive information is not unwittingly disclosed or software distributed to unauthorized persons."

During our review, we determined the current policy, ENT-SEC-140, is ambiguous and contains references to guidelines and administrative rules that do not address the policy requirement.

- Current policy requires "all agency data must be removed from the computer in such a manner that it cannot be recovered." The policy further requires "all information contained on a hard drive must be removed in such a way that meaningful information cannot be recovered from it." The policy is inconsistent within itself.
- Current policy refers to a 1996 state policy as its origin. The 1996 policy requires all computers transferred to the State's surplus property program to have appropriate certification of data removal attached to the computer. Current policy does not

require certification. In addition, the current policy does not mention the replacement of the 1996 policy so two policies exist.

- Current policy refers to laws, rules (ARMs) and standard operating procedures and applicable policies. The reference to the ARMs refers to rules on telecommunications and is not applicable when addressing computer disposal requirements.
- Current policy includes "guidelines" (defined as recommendations, not requirements) that contradict the policy requirement. These guidelines recommend tools as accepted products to meet the requirements for non-recoverable data removal. However, agencies following policy guidelines may not be in compliance with the policy requirement on data recovery, as discussed below.

Is the Computer Disposal Policy Effective?

To test the effectiveness of the current computer disposal policy, we acquired eighteen hard drives from computers no longer needed for state business, which had been transferred to either surplus property or to OPI. We examined the hard drives of each computer to determine whether all the data had been successfully removed in such a manner that it cannot be recovered. Twelve of the eighteen drives we examined, originating from eight state agencies, did not meet the policy requirement on data removal.

The following summarizes this information demonstrating why privacy is at risk.

Our review included the following information:

- Twelve of eighteen computers held information specific to a department.
  - Legal hearing notes and memos
  - Department staff communications
  - Software (violating state licensing agreements)
  - Permit applications and applicant information
  - Citizen emails to department staff
  - Department meeting notes
- Eight of eighteen computers held citizens' or business entities' private information.

- 386 social security numbers
- 182 private-party financial records
- 84 private-party business records
- Credit card numbers
- Health and medical information
- Restricted federal information
- Job applicant information
- State employee personnel information
- Department confidential procedures (security related)

Following our review, we contacted those agencies on whose original hard drives we recovered data. We determined whether personnel were aware of the state policy requirement, and what their procedures are for data removal. We determined all agencies were aware of the current policy and two were also aware of the certification requirement but not sure where the requirement came from (1996 policy). All agencies were using one of the tools suggested in the current policy guidelines. According to Department of Administration personnel, the guidelines provided in current policy have been written for varying levels of security based on data sensitivity. As a result, some suggested tools provide more protection than others. Agencies using a suggested tool assumed they were complying with state policy by making data unreadable when in fact; the tool used did not remove agency data "in such a manner that it cannot be recovered."

Summary

Removing all information from computers no longer needed for state business is an effective method enabling the state to meet its information privacy responsibilities. The guidelines currently referred to in policy include both data wiping and disk reformatting tools. The benefit of wiping data from a hard drive over reformatting the drive is the level of data recoverability allowed by each. The amount of manual user time required to perform either action is roughly the same-minutes. No manual intervention is required once the data wiping process begins. The system time is longer because it

actually overwrites data space rather than simply deleting an index file, which leaves the data intact.

The state lacks a single clear policy instructing departments on information removal, assigning responsibility for defining "sensitive data," and assigning responsibility for performing data removal and certifying the task has been completed in accordance with state policy.

State law assigns the following data security responsibilities:

> MCA 2-15-114 (enacted in 1987) states that each department head is responsible for ensuring an adequate level of security for data within the department.
>
> MCA 2-17-534 (enacted in 1987) requires the Department of Administration to establish and maintain the minimum-security standards and policies to implement 2-15-114, MCA.

Recommendation #1

We recommend the Department of Administration coordinate with the department heads and

A. Strengthen the computer disposal policy (policy) to remove all data and software in such a manner that it cannot be recovered.

B. Strengthen existing policy to require departments to certify data removal.

C. Remove guidelines from policy requirements.

D. Communicate policy to department heads.

Agency Response

DEPARTMENT OF ADMINISTRATION
DIRECTOR'S OFFICE

BRIAN SCHWEITZER, GOVERNOR

MITCHELL BUILDING

STATE OF MONTANA

(406) 444-2032
FAX 444-2812

PO BOX 200101
HELENA, MONTANA 59620-0101

May 9, 2005

RECEIVED
MAY 0 9 2005
LEGISLATIVE AUDIT DIV.

Tori Hunthausen
Deputy Legislative Auditor
Legislative Audit Division
PO Box 201705
Helena, MT 59620-1705

Dear Ms. Hunthausen:

You requested the department provide a written response to the audit report for the published report. Our response is as follows:

Disposal of Computers Policy (ENT-SEC-140)
Audit Response

The department agrees with the audit recommendations related to this policy. Privacy of data and complying with software licensing conditions are of utmost importance to the department and the State of Montana.

Revisions to the policy will be prepared that address the following:

1. Ambiguous language in the policy will be resolved.
    a. The resulting language will require that all data must be irretrievably removed from the hard drive.
    b. Likewise, only operating system software may be retained on the computer. Other software that is transferable must be reinstalled from original media provided with the surplus computer.
2. Agencies disposing of computers through any method will be required to notify the department of specific machines that have been processed for disposition. Information to be provided will include, but is not limited to, appropriate identifying information, disposition channel, "cleaning" process employed, date processed, and the agency employee performing the necessary tasks.
3. "Guidelines" will be removed from the policy to avoid any misunderstanding. A reference to the state's software standards database will be provided to readily identify the products that are allowed to perform the disposal processing. The department will assure that products listed as standard will effectively perform the data removal task.

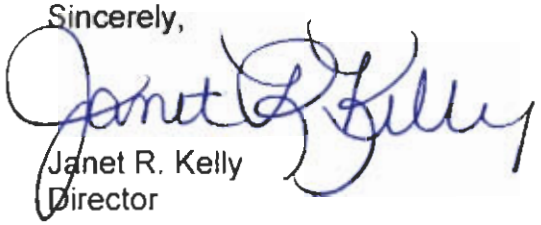
AN EQUAL OPPORTUNITY EMPLOYER

4. The existing policy setting process contains an advisory step involving the Information Technology Advisory Council (ITMC) and the Network Managers' Group (NMG). These groups are excellent avenues to distribute the finished policy, as well as publication on the policies web page that is accessible through the MINE portal under the Information Technology menu choice. Additional notification to agency non-IT senior management will ensure that agencies are aware of the updated policy.

Due to the critical nature of the audit finding, the department will expedite the revision of this policy.

We are returning your copy of the report with this response.

Sincerely,



Janet R. Kelly
Director

Enclosure
c: Jeff Brandt